

**REMARKS**

The original application upon which the accompanying Continued Prosecution Application (CPA) is based contained and continues with claims 1-20. Summarizing with respect to the amendments made herein, the amendments to the specification, FIG. 3, and claims 8 and 18 all correct clear misspellings or errors in grammar. The amendment to claim 10 replaces a mistaken use "service" with "server" and thus properly uses antecedent basis.

Accordingly, no new subject matter is added and Applicant respectfully asks that the amendments requested herein be entered.

**CONCLUSION**

In view of the foregoing, Applicant respectfully requests entry of the amendments and urges that the claims remaining in this new case are patentable. Favorable consideration is therefore requested.

Intellectual Property Law Offices  
1901 S. Bascom Ave., Suite 660  
Campbell, CA 95008

Telephone: 408.558.9950  
Facsimile: 408.558.9960  
E-mail: RRoberts@iplo.com

Customer No. 32112

Respectfully Submitted,



Raymond E. Roberts  
Reg. No.: 38,597



32112

PATENT TRADEMARK OFFICE

a

**Version with markings to show changes made**

**In the specification in the paragraph starting at page 1, line 16:**

Existing communications systems have had a long time to establish security mechanisms and to build up trust in them by their users. In the United States our conventional postal mail is a good example. We deposit our posted letters into a receptacle which is often very physically secure. Our letters are then picked up, sorted, transported, and ultimately delivered to a similar receptacle for retrieval by their recipients. Between the receptacles of a sender and a receiver the persons handling a letter are part of a single organization (at least intra-nationally) that is well known to us and considered to be highly trustworthy. Even on the rare occasions when the security of our postal system does fail, it has [mechanism] mechanisms to quickly detect and to correct this.

**In the specification in the paragraph starting at page 4, line 10:**

Accordingly, prior art cryptosystems and PKI systems provide many benefits, but even they are not perfect in all regards. It is increasingly becoming apparent [and] that it is now desirable to improve on, augment, or even replace such systems.

**In the specification in the paragraph starting at page 16, line 19:**

The text in the tables of FIG. 6a-d describes some of the particular fields, with the primary fields discussed further presently. FIG. 6a is the users table 102 of FIG. 5. This contains data records for each user, sender 12 or receiver 16, which is registered with the secure e-mail system 10. As each user registers, they are assigned a UserId (userId 102a) and they choose [an] a Password (password 102b) which are stored here. The preferred value of the Password (password 102b) is  $H(p + s)$  where p is the cleartext password and s is a salt (salt 102c) concatenated with the cleartext password. FIG. 6b is the sentMail table 104 of FIG. 5. This contains data records for each secure e-mail 14 in the secure e-mail system 10. FIG. 6c is the receivers table 106 of FIG. 5. This contains destination data for each secure e-mail 14 which is to be deliverable by the secure e-mail system 10. Since a record gets generated in this table for each receiver 16 (individual or list group) of each secure e-mail 14 that is sent, it is expected that this table will be the largest by far in the secure e-mail system 10. A null value in the FirstRequest

**Version with markings to show changes made**

field (firstRequest 106c) implies that the receiver 16 has not requested to read the secure e-mail 14. FIG. 6d is the user aliases table 103 of FIG. 5. This contains data for all known email addresses (emailAddress 103a) for each given user (userId 103b, relationally linked to userId 102a in the users table 102). Thus single users may be known by multiple email addresses, or aliases.

**In the specification in the paragraph starting at page 19, line 18:**

Here the random element is [a] an anti-cracking feature, it is a large random number used to ensure that even e-mails that are the same in content are not the same when secured; the length element is the number of characters in the body field 60; the mic element is a message integrity code created by taking a hash of the body field 60; the subject element is the contents of the subject field 58; and the body element is the contents of the body field 60.

**In the specification in the paragraph starting at page 20, line 5:**

1) If the emailAddress 103a for the sender 12 is unknown the encryption process 120 can determine a known emailAddress 103a or stop. The emailAddress 103a might be unknown for various reasons. One common example will be that the sender 12 is new to the security server 24. In this case the software module 26 can be directed to open a separate browsing window which allows the sender 12 to register on the spot. Another reason that the emailAddress 103a can be unknown is due to a user error. One simple source of such errors can be that multiple users share the same browser. A sender 12 can then be requested to clarify their identity.

**In the specification in the paragraph starting at page 24, line 20:**

In a step 166 the software module 26 validates the secure e-mail 14. This involves a second round of communications with the security server 24. The software module 26 generates new hashes of each part of the secure e-mail [14.and] 14 and sends these and the seals included in each message part to the security server 24. The security server 24 then computes new seals, based on the passed in hashes, which it compares with the passed in seals. If there are any differences, this is an indication that the secure e-mail 14 is not authentic. The security server 24 then sends an indication about the authenticity of the secure e-mail 14 back to the software

a

**Version with markings to show changes made**

module 26.

**In the specification in the paragraph starting at page 25, line 15 (add comma):**

The security features underlying the preceding encryption process 120 and decryption process 150 bear some further analysis. For authentication purposes, the operator of the security server 24 knows the sender 12 because their emailAddress 103a should associate with their password 102b. If the password 102b is treated the way it is supposed to be, i.e., only the holder should know it, then the operator of the security server 24 can be sure that only the sender 12 could have sent a particular secure e-mail 14. But the sender 12 does not necessarily even have to be trusted. By storing the sealSalt 104h initially, it is also possible for the operator of the security server 24 to be sure that no one, including the sender 12, can alter a secure e-mail 14 after it is sent. As an added security feature the sealSalt 104h may be stored encrypted in the database 100, and then never shared and never allowed to leave the security server 24. By encrypting the hashes of the body and attachments (H(b), H(a)) with the SSL key after the sender 12 has been authenticated (by providing the password 102b) it is possible to determine that it is the sender 12 who is signing their secure e-mail 14. Because the security server 24 stores only a hash of the actual password of the sender 12 as the password 102b, there is no way even the operator of the security server 24 can falsely sign a secure e-mail 14 on behalf of the sender 12.

**In the specification in the paragraph starting at page 28, line 1:**

The present secure e-mail system 10 is well suited for application in current network environments such as the Internet. The Internet, in particular, has been widely regarded as a wild frontier, largely untamed and unregulated, and where one should proceed with caution. It is also widely considered to be an environment where rapid change, limited understanding, and poor implementations of technology have left even [the] those presumably best prepared at risk. Regardless of the extent to which these concerns are actually true, it is incontestable that there is an existing and growing crises of confidence when it comes to the security of communications via the Internet. The present invention particularly addresses one key segment of such network communications, e-mail security.

a

**Version with markings to show changes made**

**In the claims:**

8 (Amended). The method of claim 1, wherein:

said step (e) includes mailing to at least one said receiver which is in a receiver list; and the method further comprising:

resolving said receiver list into a plurality of said receiver ids for said security server, to allow said security server to provide said message key to instances of said receivers which are members of said receiver list.

10 (Amended). The method of claim 1, wherein at least one of said steps (b) and (c) employs secure socket layer protocol in communications with said security [service] server.

18 (Amended). The method of claim 11, wherein:

the secure e-mail [~~was~~ is] sent by a sender and a first message seal based on the secure e-mail before it left control of said sender is stored by said security server;  
said step (b) further includes also providing to said security server a second message seal which is taken from the secure e-mail as received by said receiver; and  
said step (c) includes receiving an indication from said security server whether said first message seal and said second message seal match, to determine whether the secure e-mail was altered in transit.

*a*

Version with markings to show changes made

In the drawings:

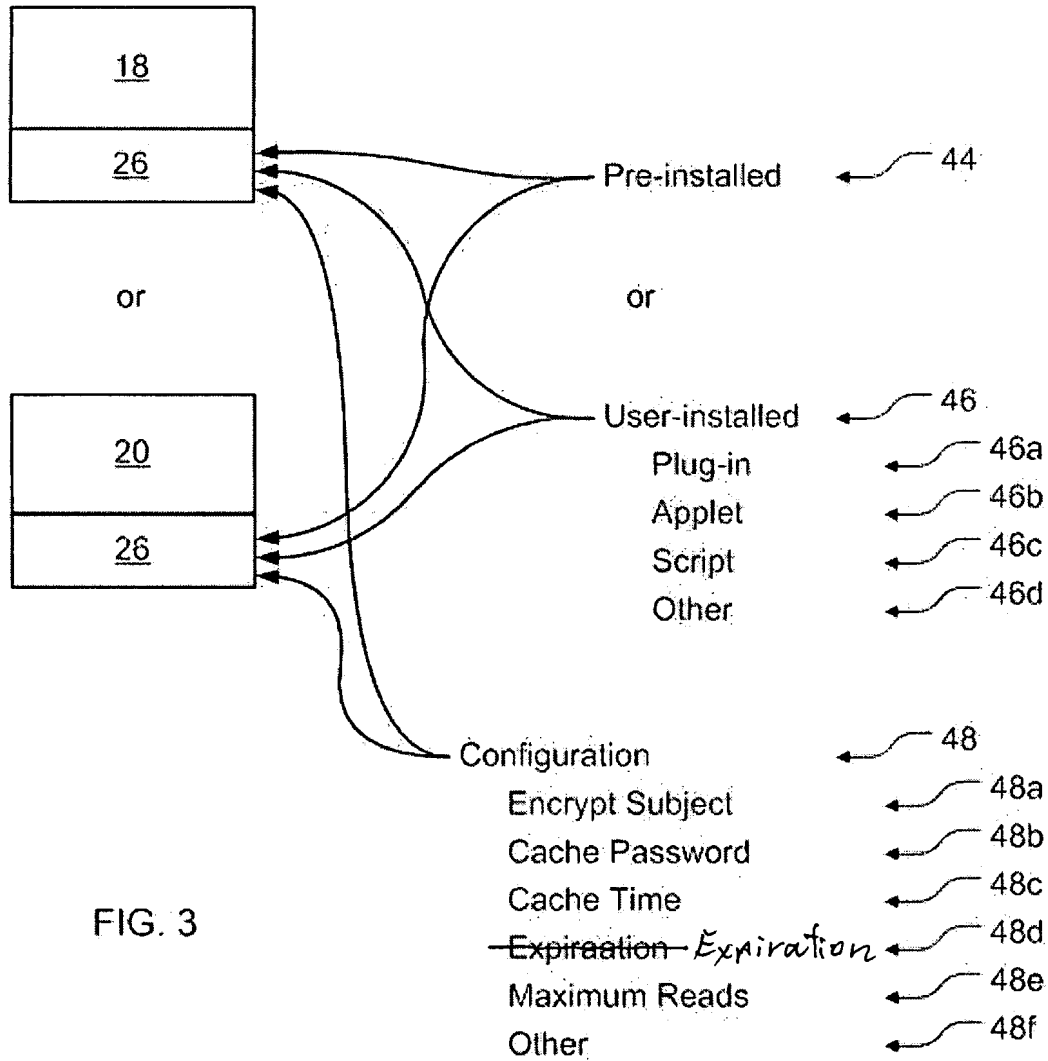


FIG. 3

a